Chapter 5
Flawed Security of Social Network of Things

Rohit Anand
G.B.Pant Engineering College, India

Akash Sinha
National Institute of Technology Patna, India

Abhishek Bhardwaj
G.B.Pant Engineering College, India

Aswin Sreeraj
G.B.Pant Engineering College, India

ABSTRACT

This chapter deals with the security flaws of social network of things. The network of things (NoT) is a dynamic structure that is basically an interface of real world and virtual world having capabilities of collection and sharing data over a shared network. The social network of things (SNoT) is a versatile way of connecting virtual and real world. Like any other device connected to internet, objects in SNoT are also vulnerable to the various security and privacy attacks. Generally, to secure Social Network of Things in which human intervention is absent, data capturing devices must be avoided. Types of security attacks that are huge threats to NoT as well as SNoT will be discussed in the chapter. The huge collection of information without necessary security measures allows an intruder to misuse the personal data of owner. Different types of attacks with reference to the different layers are also discussed in detail. The best possible potential solutions for the security of devices in SNoT will be considered.

INTRODUCTION

The Network of Things is basically internetworking of physical devices embedded with different sensors, actuators and network connectivity which enable these objects to collect and share data over and again. These devices are provided with some special sensors to perform some specific task. The Network of

DOI: 10.4018/978-1-5225-4100-4.ch005

Things (NoT) allows an object to be sensed or controlled remotely across a network established by connecting different objects (Atzori, Iera, & Morabito, 2010). This also creates an opening to establish a relation between the physical world and artificial world. When the Network of Things grows, it becomes a more general intense case of network security that can also be used as a growing technology for smart grids, virtual power plants, smart homes and smart cities. Typically, NoT is expected to offer advanced connectivity of devices, systems, and communication that go beyond machine-to-machine (M2M) communication. These devices collect some important data using sensors and other devices and have an ability to share data. That data flows among the network of these devices and can be accessed by any of the devices. This term was coined by Kevin Ashton of Procter & Gamble.

The above concept of Network of things was discussed in as early as 1982, with a modified coke machine at Carnegie Mellon University becoming the first connected device. The concept of Network of Things became popular in 1999, at Auto-ID centre of Massachusetts Institute of Technology, Cambridge. Despite many applications and potential in the industry, there is a barrier to adopt Network of Things among industry leaders and consumers. Many of NoT devices have failed to prove their relevance in society. This is a major reason that is boarding this gap. To bridge this gap, companies must identify the value that lies in order to make these devices sounder.

In some application environments, some of the NoT devices may be integrated. The resulting paradigm is Social Network of Things. The Social Network of Things has a potential to support many novel applications and networking applications in more efficient way. The Social Network of Things can be moulded to any desired shape to achieve any desired application in more effective manner. It also increases a level of trustworthiness and security. The SNoT server encompasses network layer and application layer. SNoT devices are not the proposed solution for networking but they make a world of trillions of interconnected devices more manageable. Another term of interest is Web of Things (WoT) that is used to describe approaches, software architectural styles, and programming patterns so as to allow real-world objects to be a part of World Wide Web.

As discussed above, SNoT is a very versatile way of connecting virtual and real world but since all the data and processes are connected to the internet, there is always a possibility of getting it attacked or hacked by someone. In such a case, the data must be protected and other useful information by using some special techniques. The existing SNoT security system has many flaws resulting in the need for some modern techniques to improve this flawed network security. This can be achieved by protecting the network with firewalls and protocols but the devices that are present at the endpoint will impose major problems. Each device has its own specific task but there are some devices that are linked to each other and are discardable. It is hard to detect and fix the problem for such devices. Mainly, there are two kinds of attacks or threats presented to a network. The first one is interface attack that is collecting data from the channel. It can be done by studying the data transmission through a link. The other one is Distributed Denial-of-Service (DDoS) attack. DDoS can be carried out by hindering M2M communication (Shrivastava et al., 2010). There are basically three layers in SNoT architecture: application layer, transport layer, and perception layer. The last one is responsible for interaction with the external world. Radio Frequency Identification (RFID) and Wireless Sensor Networks (WSNs), flooding, wormhole and sewage pool, witch attack, broadcast authentication, external attack, link layer security, selective forwarding attack and HELLO flooding attack are some techniques used to attack the perception layer.